July 8, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cyber Rollup

Included in this week's summary:

Click on the Section Header to go directly to that location in the Summary

NORTH DAKOTA & REGIONAL

(U) Hackers showed us how to break into the power grid – and it was shockingly easy

(U) A Wisconsin Mom-and-Pop Shop Proves Any Small Business Could Fall Victim to Chinese Hackers

NATIONAL

(U) Wendy's: Credit card numbers disclosed in cyber attack

(U) Browse free or die? New Hampshire library is at privacy fore

(U) Hackers Can Steal Your ATM PIN from your Smartwatch or Fitness Tracker

INTERNATIONAL

(U) Uber Bugs Allowed Hackers to Gather Details on Rides, Drivers, Passengers

(U) Flaw Allowed Hackers to Deliver Malicious Images via PayPal

(U) Bart Ransomware Locks Files as Individual Password-Protected ZIP Archives

(U) Ransomware slams corporate Office 365 users with macro storm

(U) Symantec Products Affected by Multiple "as Bad as It Gets" Vulnerabilities

(U) New Malware Uses Tor to Open Backdoor on Mac OS X Systems

(U) Android Ransomware Quadrupled in the Past Year

NORTH DAKOTA & REGIONAL

(U) Hackers showed us how to break into the power grid – and it was shockingly easy

(U) A power company in the Midwest hired a group of white hat hackers known as RedTeam Security to test its defenses. Techinsider followed them around for 3 days, as they attempted to break into buildings and hack into its network, with the goal of gaining full access.

Source: (U) http://www.techinsider.io/redteam-hackers-power-grid-company-2016-4

(U) A Wisconsin Mom-and-Pop Shop Proves Any Small Business Could Fall Victim to Chinese Hackers

(U) Cate Machine and Welding found out they'd accidentally become part of a China-based hacking operation when a group of former NSA employees virtually knocked on their door.

Source: (U) http://www.inc.com/adam-levin/a-wisconsin-mom-and-pop-shop-proves-any-small-business-could-fall-victim-to-chin.html

NATIONAL

(U) Wendy's: Credit card numbers disclosed in cyber attack

(U) Wendy's, which has been investigation "unusual payment-card activity" since early this year, said that cardholder names, credit or debit card numbers and expiration dates are among data targeted in an attack on a point-of-sale system at some franchise-operated restaurants. The attack, discovered in May, had been underway since November. A separate attack, which lasted from October until it was disabled in March, compromised card numbers and other account information, but not names. The security breaches affected approximately 1,025 franchise-operated Wendy's locations in the U.S.

Source: (U) http://www.usatoday.com/story/money/2016/07/07/wendys-cyber-attack-compromised-names-card-numbers/86799940/

(U) Browse free or die? New Hampshire library is at privacy fore

(U) A small library in New Hampshire sits at the forefront of global efforts to promote privacy and fight government surveillance – to the consternation of law enforcement. The Kilton Public Library in Lebanon, a city of 13,000, last year became the nation's first library to use Tor, software that masks the location and identity of internet users, in a pilot project initiated by the Cambridge, Massachusetts-based Library Freedom Project.

Source: (U) http://bigstory.ap.org/article/72cc147dd9bb4003b29eea0b8fc3a118/browse-free-or-die-new-hampshire-library-privacy-fore

(U) Hackers Can Steal Your ATM PIN from Your Smartwatch or Fitness Tracker

(U) A recent study from Binghamton University also suggests your smartwatch or fitness tracker is not as secure as you think – and it could be used to steal your ATM PIN code. The risk lies in the motion sensors used by these wearable devices.

Source: (U) http://thehackernews.com/2016/07/hacking-smartwatch-atm.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1276.iv0ao09bj9.qp8

INTERNATIONAL

(U) Uber Bugs Allowed Hackers to Gather Details on Rides, Drivers, Passengers

(U) Uber is in the process of fixing a slew of security bugs disclosed by security firm Integrity, who discovered and reported 14 issues it found on the company's websites and mobile applications. The security firm only published details about six of these bugs, as they're waiting on Uber to patch four more.

Source: (U) http://news.softpedia.com/news/uber-bugs-allowed-hackers-to-gather-details-on-uber-rides-drivers-passengers-505663.shtml

(U) Flaw Allowed Hackers to Deliver Malicious Images via PayPal

(U) PayPal has addressed a vulnerability that could have been exploited by hackers to insert malicious images into payment pages. Security researcher Aditya K Sood discovered that the URL of payment pages set up by PayPal users included a parameter called "image_url".

Source: (U) http://www.securityweek.com/flaw-allowed-hackers-deliver-malicious-images-paypal

(U) Bart Ransomware Locks Files as Individual Password-Protected ZIP Archives

(U) After the return of the Necurs botnet and its main payload, the Locky ransomware, security experts have noticed new ransomware among all the spam the botnet spews on a daily basis. Called Bart, based on the extension it adds to locked files, the ransomware is not as sophisticated as Locky but bears some resemblance to its older brother.

Source: (U) http://news.softpedia.com/news/bart-ransomware-locks-files-as-individual-password-protected-zip-archives-505659.shtml

(U) Ransomware slams corporate Office 365 users with macro storm

(U) Spam flood tried to drop malicious macros in inboxes. Microsoft Office macros are still a viable infection vector: security outfit Avanan says it's spotted a week-long, large-scale malware attack against Office 365 users. The campaign began on June 22, and Microsoft started blocking the malicious attachment on June 23.

Source: (U) http://www.theregister.co.uk/2016/06/28/ransomware_scum_target_corporate_office_365_users_in_0day_campaign/

(U) Symantec Products Affected by Multiple "as Bad as It Gets" Vulnerabilities

(U) Tavis Ormandy, a member of Google's Project Zero initiative, has discovered a series of vulnerabilities in Symantec's security products. Due to the nature of these flaws, they affect a large number of Symantec products, and not all can be patched via automatic updates.

Source: (U) http://news.softpedia.com/news/symantec-products-affected-by-multiple-as-bad-as-it-gets-vulnerabilities-505786.shtml

(U) New Malware Uses Tor to Open Backdoor on Mac OS X Systems

(U) Security researchers from Bitdefender have discovered a new malware family that opens a backdoor via the Tor network on Mac OS X systems. The malware's technical name is Backdoor.MAC.Eleanor, and currently, its creators are distributing it to victims as EasyDoc Converter, a Mac app that allows users to convert files by dragging them over a small window.

Source: (U) http://news.softpedia.com/news/new-malware-uses-tor-to-open-backdoor-on-mac-os-x-systems-506000.shtml

(U) Android Ransomware Quadrupled in the Past Year

(U) Mobile ransomware attacks targeting Android users have grown four times compared to the same period of last year, and most of these attacks can be attributed to only four strains of Android ransomware. According to a recent Kaspersky Lab study, Android ransomware has hit 136,532 users in the 2015-2016 period, increasing from 35,413 victims recorded in the 2014-2015 period.

Source: (U) http://news.softpedia.com/news/android-ransomware-quadrupled-in-the-past-year-505818.shtml

The Bi-Weekly Cyber Roll up is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material. If you have any items that you would like to see added to the Bi-Weekly Cyber Roll up, please forward it to the NDSLIC (ndslic@nd.gov).